On some combinatorial properties of the orbits on subsets

Xavier Buchwalder

CWI Amsterdam

xpjb@cwi.nl

August 24, 2010

Abstract

We introduce generalised orbit algebras. The purpose here is to measure how some combinatorial properties can characterize the action of a group of permutations of the elements of Ω on the subsets of Ω. The similarity with orbit algebras is such that it took the author a long time to find a generalised orbit algebra not arising from a permutation group.

1 Introduction

Let Ω be a finite set and $\mathcal{P}(\Omega)$ its powerset. For every set A, we shall denote by $|A|$ the number of elements in A. We define a *strongly regular partition* of $\mathcal{P}(\Omega)$ to be any partition of $\mathcal{P}(\Omega)$ into blocs $\mathsf{B}_1, \ldots, \mathsf{B}_s$ such that :

1. The blocs contain sets of the same size.

2. For any bloc B_i, the set of all the complements of the members of B_i is also a bloc, say $\mathsf{B}_{c(i)}$.

3. For any two blocs B_i and B_j, the number of members of B_j that are included in a member A of B_i is independent of the choice of A in B_i. We denote by $\binom{\mathsf{B}_i}{\mathsf{B}_j}$ this number.

We first remark that this definition is somewhat equivalent to having a tactical decomposition between each pair of blocs. As an example, if $\Omega = \{1, 2, 3\}$, the following partition is strongly regular :

$$\emptyset \quad \{1\}, \{2\} \quad \{3\} \quad \{1,2\} \quad \{1,3\}, \{2,3\} \quad \{1,2,3\}$$

The main concern of the paper is the study of strongly regular partitions, through an algebraic point of view. A long standing question for the author was whether there exists a strongly regular partition not arising as the set of orbits

1

of a group of permutations of Ω on its powerset. This question is answered at the end of the paper.

Along the way, various results about the reconstruction conjecture in graph theory are shown to apply for strongly regular partitions. Among them the results of L.Lovász and V.Müller play a key role : our point of view is to try to explain and extend these results and the counting strategy behind them. For this purpose, we prove the following :

Lemma 1. *For any two blocs* B_i *and* B_j, *the number of members of* B_j *that contain a member* A *of* B_i *is independent of the choice of* A *in* B_i. *Moreover, this number is equal to* $\frac{\binom{\Omega}{\mathsf{B}_j}}{\binom{\Omega}{\mathsf{B}_i}}\binom{\mathsf{B}_j}{\mathsf{B}_i}$ *and to* $\binom{\mathsf{B}_{c(i)}}{\mathsf{B}_{c(j)}}$.

Theorem 1. *If* P *is a strongly regular partition, then for any two blocs* B_i *and* B_j *of* P, *the number of members of* B_j *that intersects a subset of size* r *of a given member* A *of* B_i *is independent of the choice of* A *in* B_i.

Theorem 2. *If* P *is a strongly regular partition, then for any three blocs* B_i, B_j, *and* B_k *of* P, *and any integers* $r_1, \ldots, r_4$:

$$
\left| \left\{ (A, B) \in \mathsf{B}_i \times \mathsf{B}_j \ \ s.t. \ \left\{ \begin{array}{l} |A \cap B| = r_1 \\ |A \cap C| = r_2 \\ |B \cap C| = r_3 \\ |A \cap B \cap C| = r_4 \end{array} \right\} \right\} \right|
$$

is independent of the choice of C *in* B_k.

One could have expected that these new results, and the framework that comes along would yield an improvement on the Edge Reconstruction Conjecture. A discussion of this problem is provided, including some previously unknown limit cases that establish the impossibility of improving the result of V.Müller in the general case of reconstruction under group action.

We choose the algebraic point of view for our exposition, and instead of the pair orbits-blocs, we study orbit algebras and the generalised orbit algebras corresponding to strongly regular partitions. This emphasize the role of two operators : derivation and complementation, which are shown to generate the Terwilliger algebra. This shows a link between the Terwilliger algebra and the reconstruction conjectures that was never emphasized to this degree.

2 Generalised orbit algebras

2.1 Orbit algebras

Definition 1. *We consider* $\mathcal{S}_n$ *the quotient algebra of the polynomial algebra* $\mathbb{R}[x_1, \ldots, x_n]$ *by the ideal of polynomials generated by* $x_1^2 - x_1, x_2^2 - x_2, \ldots, x_n^2 - x_n$.

To emphasize the product of $\mathcal{S}_n$, we sometimes write $p \cdot q$ instead of pq. It is clear that $\mathcal{S}_n$ is a real vector space of dimension 2^n, and that the polynomials

$$p_A = \prod_{i \in A} x_i, \text{ with } A \in \mathcal{P}(\Omega)$$

are a basis of $\mathcal{S}_n$. We observe that :

- $p_\emptyset = 1$

- $\forall (A, B) \in \mathcal{P}(\Omega)^2, \quad p_A \cdot p_B = p_{A \cup B}$

For every n, the polynomial algebra $\mathcal{S}_n$ is also an algebra of functions on $\mathcal{P}(\Omega)$ (with pointwise multiplication) :

Definition 2. *If A and B are two subsets of Ω, we define the value of p_A at the set B to be :*

$$p_A(B) = \begin{cases} 1 \text{ if } A \subseteq B \\ 0 \text{ otherwise} \end{cases}$$

As the p_A, $A \in \mathcal{P}(\Omega)$, form a basis of $\mathcal{S}_n$, we can extend the above evaluation to every polynomial of $\mathcal{S}_n$ by linearity. We call the function which maps a polynomial of $\mathcal{S}_n$ to its associated real function on $\mathcal{P}(\Omega)$ *evaluation.* It is an algebra isomorphism, as :

- For every triple (A, B, C) of subsets of Ω, $A \cup B \subseteq C$ if and only if $A \subseteq C$ and $B \subseteq C$, hence $p_A \cdot p_B(C) = p_{A \cup B}(C) = p_A(C) p_B(C)$.

- If $p = \sum_{A \subseteq \Omega} \alpha_A p_A$ is such that for every subset B of Ω $p(B) = 0$, then p is identically 0. To prove this, we consider a subset C of Ω such that $\alpha_C \neq 0$ and $|C|$ is maximal for this property. Then we would have $p(C) = 0$ and $p(C) = \alpha_C$.

This isomorphism indicates that Lagrange interpolation can be used, and we shall use it to deduce our first structure theorem concerning the subalgebras of $\mathcal{S}_n$:

Theorem 3. *For every subalgebra $\mathcal{A}$ of $\mathcal{S}_n$ that contains 1, there exists a partition P of $\mathcal{P}(\Omega)$ such that :*

$$\mathcal{A} = \left\{ p \in \mathcal{S}_n \quad s.t. \quad \forall \mathsf{P}_i \in \mathsf{P} \quad \forall (A, B) \in \mathsf{P}_i^2 \quad p(A) = p(B) \right\}$$

Proof. For every polynomial p, we define an equivalence relation on $\mathcal{P}(\Omega)$ by :

$$A \mathcal{R}_p B \Leftrightarrow p(A) = p(B)$$

This relation partitions $\mathcal{P}(\Omega)$ into generalised orbits $\mathsf{P}_1, \ldots, \mathsf{P}_s$, corresponding to distinct values of p. We put

$$r_i = \frac{\prod_{T \notin \mathsf{P}_i} (p - p(T))}{\prod_{T \notin \mathsf{P}_i} (p(A) - p(T))} \quad \text{for some } A \in \mathsf{P}_i$$

and observe that $r_i(B)$ is 1 if B is a member of P_i and 0 otherwise. Also, each r_i is in $\mathcal{A}$. If we consider the total relation, that is

$$A \mathcal{R} B \Leftrightarrow p(A) = p(B), \ \forall p \in \mathcal{A}$$

then $\mathcal{R}$ partitions $\mathcal{P}(\Omega)$ into generalised orbits $\mathsf{Q}_1, \ldots, \mathsf{Q}_s$, and we see that

$$\mathcal{A} \subseteq \left\{ p \ \in \mathcal{S}_n \quad s.t. \quad \forall i = 1 \ldots s, \ \forall (A, B) \in \mathsf{Q}_i^2 \quad p(A) = p(B) \right\}$$

As for the reverse inclusion, there exists a polynomial ε_i in $\mathcal{A}$ such that $\varepsilon_i(A)$ is 1 if A is a member of Q_i and 0 otherwise : we consider the product of some of the r_i defined above. The isomorphism between $\mathcal{S}_n$ and real functions on $\mathcal{P}(\Omega)$ allows us to conclude that any polynomial that takes constant values on each of the Q_i is a linear combination of the ε_i, that is to say, is in $\mathcal{A}$. $\qquad\square$

We observe that, conversely, any partition P of $\mathcal{P}(\Omega)$ uniquely defines a subalgebra of $\mathcal{S}_n$ containing 1, namely :

$$\left\{ p \ \in \mathcal{S}_n \quad s.t. \quad \forall \mathsf{P}_i \in \mathsf{P} \quad \forall (A, B) \in \mathsf{P}_i^2 \quad p(A) = p(B) \right\}$$

and deduce that there is a finite number of subalgebras of $\mathcal{S}_n$: exactly as many as there are partitions of $\mathcal{P}(\Omega)$.

The group of permutations $\mathfrak{S}_n$ of the elements of Ω acts on $\mathcal{S}_n$ as a group of algebra isomorphisms defined by :

$$\sigma \cdot x_i = x_{\sigma(i)} \ , \ \sigma \ \in \ \mathfrak{S}_n$$

Definition 3. *For every subgroup Γ of $\mathfrak{S}_n$, the set*

$$\mathcal{S}_n^\Gamma = \{ p \in \mathcal{S}_n \quad s.t. \quad \sigma \cdot p = p \quad \forall \sigma \in \Gamma \}$$

is a subalgebra of $\mathcal{S}_n$ called the orbit algebra *of Γ. Its elements are called the* invariants *of Γ. If an algebra $\mathcal{A}$ is equal to $\mathcal{S}_n^\Gamma$ for some subgroup Γ of $\mathfrak{S}_n$, we will say that $\mathcal{A}$ is an* orbit algebra.

The above considerations yield a natural enumeration of the subalgebras of $\mathcal{S}_n$ as a bijection with the partitions of $\mathcal{P}(\Omega)$, and we would like to obtain a combinatorial characterization of subalgebras of $\mathcal{S}_n$ that are orbit algebras, or equivalently, of partitions of $\mathcal{P}(\Omega)$ that are the orbits of a subgroup Γ of $\mathfrak{S}_n$.

To conclude with orbit algebras, we remark that two distinct groups do not necessarily yield the same orbit algebra but it is nevertheless almost always true for primitive permutation groups, according to a theorem of [4].

2.2 Generalised orbit algebras

Definition 4. • *We call* derivation *the linear mapping ∂ of $\mathcal{S}_n$ to itself defined by :*

$$\partial(p_A) = \sum_{i \in A} p_{A \setminus i}, \quad \forall A \subseteq \Omega$$

- *We call* complementation *the linear mapping* $\complement$ *of* $\mathcal{S}_n$ *to itself defined by* :

$$\complement(p_A) = p_{\Omega \setminus A}, \quad \forall A \subseteq \Omega$$

We have for example that $\partial(p_\emptyset) = \partial(1) = 0$, and that $\complement(p_\emptyset) = \complement(1) = p_\Omega$. Also, if $n \geq 2$, $\partial(p_{\{1,2\}}) = p_{\{1\}} + p_{\{2\}}$.

It is clear that complementation is an involution, that is to say $\complement \circ \complement$ is the identity of $\mathcal{S}_n$. As for ∂, one can show that for any integer k and any subset A of Ω,

$$\partial^k(p_A) \quad = \quad \sum_{\substack{B \subseteq A \\ |B| = |A| - k}} k! p_B \tag{1}$$

Hence, ∂ is nilpotent of order $n + 1$.

One can show that for every permutation σ in $\mathfrak{S}_n$, and every pair p, q of polynomials in $\mathcal{S}_n$, one has :

- $\sigma(p \cdot q) = \sigma(p) \cdot \sigma(q)$

- $\sigma \circ \partial(p) = \partial \circ \sigma(p)$

- $\sigma \circ \complement(p) = \complement \circ \sigma(p)$

We deduce that any orbit algebra is closed under derivation, complementation and multiplication. This is underlying numerous results about orbit algebras and orbits on subsets as the Livingstone-Wagner theorem [8] : the number of orbits on $k + 1$-subsets is at least the number of orbits on k-subsets if $k < \frac{n}{2}$. Also, the orbits on k-subsets are determined independently of the group by the orbits on $k + 1$-subsets in this case, that is to say the restriction of ∂ to the orbits of size $k + 1$ is surjective if $k < \frac{n}{2}$, and also injective if $k \geq \frac{n}{2}$. A simple proof is provided below.

For instance, if $n = 3$, one can consider the real vector space on

$$\{1, \ x_1 + x_2, \ x_3, \ x_1 x_2, \ x_1 x_3 + x_2 x_3, \ x_1 x_2 x_3\}$$

which is the orbit algebra of the subgroup $\{\mathrm{Id}, (12)(3)\}$. It is closed under multiplication, and we have :

$$
\begin{array}{rclcrcl}
\partial(1) & = & 0 & \qquad & \complement(1) & = & x_1 x_2 x_3 \\
\partial(x_1 + x_2) & = & 2 & & \complement(x_1 + x_2) & = & x_1 x_3 + x_2 x_3 \\
\partial(x_3) & = & 1 & & \complement(x_3) & = & x_1 x_2 \\
\partial(x_1 x_2) & = & x_1 + x_2 & & \complement(x_1 x_2) & = & x_3 \\
\partial(x_1 x_3 + x_2 x_3) & = & x_1 + x_2 + 2x_3 & & \complement(x_1 x_3 + x_2 x_3) & = & x_1 + x_2 \\
\partial(x_1 x_2 x_3) & = & x_1 x_2 + x_1 x_3 + x_2 x_3 & & \complement(x_1 x_2 x_3) & = & 1
\end{array}
$$

It has been a long standing question for the author to find out whether there are subspaces of $\mathcal{S}_n$ closed under derivation, complementation and multiplication that are not the orbit algebras of a group of permutations. Computer aided enumeration indicates that they do not exist with $n \leq 6$. This question motivated the following developments.

Definition 5. *A* generalised orbit algebra *is a nonempty nonzero subalgebra of $\mathcal{S}_n$ that is closed under derivation and complementation. To emphasize the parameter n, we might say that a generalised orbit algebra has* order n.

As generalised orbit algebras are particular subalgebras of $\mathcal{S}_n$ (we will see that they always contain 1), one might consider their associated partition defined by Theorem 3. That is to say, given a generalised orbit algebra $\mathcal{D}$, the subsets of the set $\mathcal{P}(\Omega)$ on which every polynomial of $\mathcal{D}$ take the same value. For the above example, one can see that the generalised orbits of the associated partition are :

$$\emptyset \quad \{1\}, \{2\} \quad \{3\} \quad \{1,2\} \quad \{1,3\}, \{2,3\} \quad \{1,2,3\}$$

It is a remarkable fact (for a subalgebra of $\mathcal{S}_n$), that there is a natural bijection between the generalised orbits of this partition and the polynomial basis we took for this particular algebra. This is indeed true of any orbit algebra[1], and more generally, of any generalised orbit algebra. In the following, we develop a formal algebraic machinery which can be applied to establish this fact (although generalised orbit algebras are not the only algebras satisfying this property).

Definition 6. *We denote by l the linear mapping of $\mathcal{S}_n$ to itself defined by :*

$$l(p) = \sum_{k=0}^{n} \frac{\partial^k(p)}{k!}$$

Observing the equation (1), one can see that $\forall A \subseteq \Omega$,

$$l(p_A) = \sum_{B \subseteq A} p_B$$

The powers of l have a neat expression in terms of ∂ :

Lemma 2 (Mnukhin [13]). *For every nonzero integer m :*

$$l^m = \sum_{k=0}^{n} \frac{m^k}{k!} \partial^k$$

Proof. If r and s are nonzero integers, one has :

$$
\begin{aligned}
\left(\sum_{k=0}^{n} \frac{r^k}{k!} \partial^k \right) \circ \left(\sum_{i=0}^{n} \frac{s^i}{i!} \partial^i \right) &= \sum_{k=0}^{n} \sum_{i=0}^{n} \frac{r^k s^i}{k! i!} \partial^{k+i} \\
&= \sum_{m=0}^{2n} \partial^m \sum_{k=0}^{m} \frac{r^k s^{m-k}}{k!(m-k)!} \\
&= \sum_{m=0}^{n} \frac{\partial^m}{m!} \sum_{k=0}^{m} \frac{m!}{k!(m-k)!} r^k s^{m-k} \\
&= \sum_{m=0}^{n} \frac{(r+s)^m}{m!} \partial^m
\end{aligned}
$$

---

[1]i.e. the orbits of a group Γ on $\mathcal{P}(\Omega)$ index a basis of the orbit algebra of Γ, and form the partition associated with $\mathcal{S}_n^{\Gamma}$ by Theorem 3.

As the Lemma is true if $m = 1$, the above equality provides a proof of the property for $m > 0$, by induction. One can use the same computations with $r = -1$ and $s = 1$ to show that :

$$\left(\sum_{k=0}^{n} \frac{(-1)^k}{k!} \partial^k \right) \circ l = Id$$

The Lemma is then true if $m = -1$, and thus if $m < 0$ by induction. □

This Lemma implies that l is an isomorphism, and by using a VanderMonde matrix, we see that there exist rational numbers $a_1, \ldots, a_{n+1}$ such that :

$$\partial = \sum_{r=1}^{n+1} a_r l^r \tag{2}$$

Definition 7. *We denote by ε the linear mapping of $\mathcal{S}_n$ to itself defined by :*

$$\varepsilon(p) = \mathsf{C} \circ l^{-1} \circ \mathsf{C}(p)$$

Moreover, we shall use the simplified notation $\varepsilon_A = \varepsilon(p_A)$ for any subset A of Ω.

The mapping ε is an isomorphism, hence $\{\varepsilon_A \; : \; A \subseteq \Omega\}$ is a basis of $\mathcal{S}_n$. By equation (1), and Lemma 2 we have :

$$\varepsilon_A = \sum_{B \supseteq A} (-1)^{|B|-|A|} p_B \tag{3}$$

Lemma 3. $\varepsilon_A(B) = 1$ *if* $A = B$ *and 0 otherwise .*

Proof.

$$\begin{aligned}
\varepsilon_A(B) &= \sum_{C \supseteq A} (-1)^{|C|-|A|} p_C(B) \\
&= (-1)^{|A|} \sum_{C \ s.t. \ A \subseteq C \subseteq B} (-1)^{|C|} \\
&= \begin{cases} 1 \ if \ A = B \\ 0 \ if \ A \neq B \end{cases}
\end{aligned}$$

□

Due to the existence of the isomorphism between $\mathcal{S}_n$ and the real functions on $\mathcal{P}(\Omega)$, one can see that the ε_A form a basis of idempotents of $\mathcal{S}_n$, that is $\varepsilon_A \cdot \varepsilon_B = \varepsilon_A$ if $A = B$ and 0 otherwise. The idea of constructing the idempotents in this way is well known, for example in [12]. We immediately deduce the following :

Corollary 1. *Let $\mathcal{F}$ be the algebra of real-valued functions on $\mathcal{P}(\Omega)$ with point-wise multiplication. The following map is an algebra isomorphism between $\mathcal{F}$ and $\mathcal{S}_n$:*

$$\theta \; : \; f \mapsto \sum_{A \subseteq \Omega} f(A)\varepsilon_A$$

Moreover, θ is the inverse of the evaluation map.

Proof. According to Lemma 3, the evaluation of $\theta(f)$ is f. $\qquad\square$

This is very useful for computing products in $\mathcal{S}_n$. In the following, we develop the link between the polynomials ε_A and the partition structure, but first we prove that every generalised orbit algebra contains 1, and more precisely, that every generalised orbit algebra contains a particular subspace : the orbit algebra of $\mathfrak{S}_n$.

Lemma 4. *Every generalised orbit algebra $\mathcal{D}$ contains the following polynomials :*

$$\sum_{A \; s.t. \; |A|=k} p_A, \quad k \in \{0\dots n\}$$

Proof. $\mathcal{D}$ being a generalised orbit algebra, there exists

$$p = \sum_{A \subseteq \Omega} \alpha_A \varepsilon_A \neq 0 \ \in \mathcal{D}$$

As we have seen, the ε_A are idempotents, thus :

$$p^2 = \sum_{A \subseteq \Omega} \alpha_A^2 \varepsilon_A \in \mathcal{D}$$

and ε is a linear isomorphism, so :

$$\varepsilon^{-1}(p^2) = \sum_{A \subseteq \Omega} \alpha_A^2 p_A \in \mathcal{D}$$

Now if we let $k = max\,\{r \; / \; \exists A \subseteq \Omega \; s.t. \; |A| = r \; and \; \alpha_A \neq 0\}$, then

$$\partial^k \circ \varepsilon^{-1}(p^2) = \underbrace{\left(\sum_{A \subseteq \Omega \; s.t. \; |A|=k} k!\alpha_A^2 \right)}_{\neq 0} p_\emptyset \in \mathcal{D}$$

We have $1 = p_\emptyset \in \mathcal{D}$, and $\mathcal{D}$ is closed under complementation, so $p_\Omega \in \mathcal{D}$. We conclude by noting that :

$$\frac{1}{s!}\partial^s(p_\Omega) = \sum_{A \; s.t. \; |A|=n-s} p_A, \quad s \in \{0\dots n\}$$

$\qquad\square$

We now emphasize the link between the partition associated to a generalised orbit algebra by Theorem 3 with a natural basis of this generalised orbit algebra.

Definition 8. *A* generalised orbit *of a generalised orbit algebra $\mathcal{D}$ is a nonempty subset* B *of $\mathcal{P}(\Omega)$ such that*

1.

$$\sum_{A \in \mathsf{B}} p_A \in \mathcal{D}$$

2. B *is minimal with respect to this property :*

$$\forall\ \mathsf{B}' \subsetneq \mathsf{B},\ \mathsf{B}' \neq \emptyset \quad \sum_{A \in \mathsf{B}'} p_A \notin \mathcal{D}$$

It is clear that two different generalised orbits B_1 and B_2 of $\mathcal{D}$ are disjoint, because if not, any generalised orbit algebra being closed under ε, $\mathsf{B}_1 \cap \mathsf{B}_2$ would be a generalised orbit of $\mathcal{D}$, as :

$$\left(\sum_{A \in \mathsf{B}_1} \varepsilon_A\right)\left(\sum_{B \in \mathsf{B}_2} \varepsilon_B\right) = \sum_{C \in \mathsf{B}_1 \cap \mathsf{B}_2} \varepsilon_C$$

This cannot happen, because B_1 and B_2 are minimal. The same argument shows that the set of all subsets B of $\mathcal{P}(\Omega)$ such that $\sum_{A \in \mathsf{B}} p_A \in \mathcal{D}$ is closed under intersection. Moreover, we have already seen[2] that the polynomials $\sum_{A\ s.t.\ |A|=k} p_A,\ k \in \{0 \ldots n\}$, are in $\mathcal{D}$, thus any subset of Ω is in a generalised orbit. We conclude that the generalised orbits of a generalised orbit algebra form a partition of $\mathcal{P}(\Omega)$.

Theorem 4. *Let $\mathcal{D}$ be a generalised orbit algebra, and $\mathsf{B}_1, \ldots, \mathsf{B}_s$ the partition of $\mathcal{P}(\Omega)$ associated to $\mathcal{D}$ by Theorem 3, that is :*

$$\mathcal{D} = \left\{ p\ \in \mathcal{S}_n \quad s.t. \quad \forall i = 1 \ldots s \quad \forall (A,B) \in \mathsf{B}_i^2 \quad p(A) = p(B) \right\}$$

Then :

1. *The associated set of polynomials $\varepsilon_{\mathsf{B}_i} = \sum_{A \in \mathsf{B}_i} \varepsilon_A$ is a basis of $\mathcal{D}$ as a real vector space.*

2. *The associated set of polynomials $p_{\mathsf{B}_i} = \sum_{A \in \mathsf{B}_i} p_A$ is a basis of $\mathcal{D}$ as a real vector space.*

3. *The generalised orbits of $\mathcal{D}$ are the sets $\mathsf{B}_1, \ldots, \mathsf{B}_s$.*

Proof. 1. The $\varepsilon_A,\ A \subseteq \Omega$, constitute a basis of $\mathcal{S}_n$ which contains $\mathcal{D}$, and the B_i are disjoint, so the family is independent. If we consider an element p of $\mathcal{D}$, we have, by Corollary 1 :

$$p = \sum_{A \subseteq \Omega} p(A)\varepsilon_A$$

Thus the family also generates $\mathcal{D}$.

---

[2]in Lemma 4

2. As ε is invertible, ε^{-1} maps any basis of $\mathcal{D}$ to another basis of $\mathcal{D}$.

3. If $\sum_{A \in \mathsf{B}} p_A \in \mathcal{D}$ with $\mathsf{B} \subseteq \mathsf{B}_i$ for some i, then if we put $q = \sum_{A \in \mathsf{B}} \varepsilon_A$, q belongs to $\mathcal{D}$. Suppose that there exists both $C \in \mathsf{B}_i \setminus \mathsf{B}$ and $D \in \mathsf{B}$. We would have $q(C) = 0$ and $q(D) = 1$, which would be a contradiction to the definition of B_i.

$\square$

Various properties of this *generalised orbit system* follow from Theorem 3. For instance, if $\mathcal{D}_1$ and $\mathcal{D}_2$ are two generalised orbit algebras such that $\mathcal{D}_1 \subseteq \mathcal{D}_2$, then the generalised orbits of $\mathcal{D}_2$ are a refinement of those of $\mathcal{D}_1$. According to Lemma 4, the generalised orbits of any generalised orbit algebra are a refinement of those of $\mathcal{S}_n^{\mathfrak{S}_n}$, which means that all the sets in a generalised orbit B have the same size $\sharp \mathsf{B}$.

Generalised orbit algebras share the property of being closed under ε with orbit algebras, that is, their generalised orbit system index one of their basis. From equation (2), we infer that generalised orbit algebras are exactly the nonempty and nonzero subalgebras of $\mathcal{S}_n$ that are closed under ε and $\complement$. For an example of an algebra closed under ε but not $\complement$, one may consider the vector space spanned by :

$$\left\{ p_\emptyset, \ p_{\{1\}} + p_{\{2\}}, \ p_{\{3\}}, \ p_{\{1,2\}}, \ p_{\{1,3\}}, \ p_{\{2,3\}}, \ p_{\{1,2,3\}} \right\}$$

This basis is indexed by the generalised orbits of the partition given by Theorem 3 in a very natural way.

An important property of orbit algebras, and of the orbits of a permutation group on $\mathcal{P}(\Omega)$, is that the inclusion relations, and the stronger intersection relations have nice properties : for example, the number of elements of an orbit O_1 that intersects a subset of size r of a set A depends only on the orbit O_2 of A, and not on A itself. In the following, we embark on a systematic study of such properties, our hope being to generalize them to generalised orbit algebras.

Definition 9. *We denote by $Com(\mathfrak{S}_n)$ the set of linear functions h from $\mathcal{S}_n$ to itself such that :*

$$\forall \sigma \in \mathfrak{S}_n, \ h \circ \sigma = \sigma \circ h$$

Given two pairs of subsets (A_1, A_2) and (B_1, B_2) of Ω, one can see that there exists a permutation in $\mathfrak{S}_n$ that simultaneously maps A_1 to B_1 and A_2 to B_2 if and only if :

- $|A_1| = |B_1|$

- $|A_2| = |B_2|$

- $|A_1 \cap A_2| = |B_1 \cap B_2|$

We deduce that the mappings

$$E_{k,l,r} : p_A \mapsto \begin{cases} \sum_{\substack{B \ s.t \ |B| = l \\ |A \cap B| = r}} p_B & \text{if } |A| = k \\ 0 & \text{otherwise} \end{cases}$$

where k, l, r are non-negative integers such that $r \leq k$, $r \leq l$, $k + l - r \leq n$, form a basis of $\text{Com}(\mathfrak{S}_n)$. As an example, if k is an integer between 0 and n, we shall denote by id_k the function $E_{k,k,k}$ which maps a polynomial p_A to itself if $|A| = k$, and to 0 otherwise.

We observe that every orbit algebra is closed under any mapping in $\text{Com}(\mathfrak{S}_n)$. We will show that this is indeed true for any generalised orbit algebra with the following :

Theorem 5. *$\text{Com}(\mathfrak{S}_n)$ is generated by ∂ and C as a real algebra under composition of mappings.*

We point out to the reader that $\text{Com}(\mathfrak{S}_n)$ is known as the Terwilliger algebra of the hypercube, and have already been the object of intensive study (see [6]), with surprising applications (for example [15]). We independently provide here a set of generators that is more convenient for our purposes.

Proof. We will prove by induction that for every integer k between 0 and $\frac{n}{2}$, the $E_{u,v,w}$ where either $u \leq k$ or $v \leq k$ can be generated by ∂ and C, by composition, and by taking real linear combinations.

- If $k = 0$, we see that for every integer l :

$$\partial^{n-l} \circ \mathsf{C} \circ \partial^n \circ \mathsf{C} = n! \, (n-l)! E_{0,l,0}$$

$$\partial^l \circ E_{0,0,0} = l! E_{l,0,0}$$

- Suppose that for every integer l less than $k \leq \frac{n}{2}$, we can generate all the $E_{u,v,w}$, with either $u \leq l$ or $v \leq l$. Note that :

$$\partial^{n-2k} \circ \mathsf{C} = (n - 2k)! \sum_{r=0}^{2k} E_{r,2k-r,0}$$

This allows us to construct $E_{k,k,0}$ as the only member of the right hand side not already addressed by the induction hypothesis. By means of a right composition, we can generate the :

$$E_{k-1,k,t} \circ \partial = E_{k,k,t} + E_{k,k,t+1}, \quad t = 0 \dots k-1 \tag{4}$$

By induction, we construct $E_{k,k,t+1}$ for $t = 0 \dots, k-1$. In particular, $id_k = E_{k,k,k}$ is generated. To conclude, we observe that :

$$\mathsf{C} \circ \partial^{v-r} \circ \mathsf{C} \circ \partial^{u-r} \circ id_u = (u-r)!(v-r)! \sum_{w=r}^{\min(u,v)} \binom{w}{r} E_{u,v,w} \tag{5}$$

and that this is equal to

$$id_v \circ \mathsf{C} \circ \partial^{v-r} \circ \mathsf{C} \circ \partial^{u-r} = (u-r)!(v-r)! \sum_{w=r}^{\min(u,v)} \binom{w}{r} E_{u,v,w} \tag{6}$$

For any u and v with either $u \leq k$ or $v \leq k$, we can now retrieve the $E_{u,v,w}$, $w = 0 \dots \min(u,v)$ by a triangular linear system.

11

$\square$

As previously mentioned, any generalised orbit algebra is therefore closed under any mapping of $\mathrm{Com}\,(\mathfrak{S}_n)$. In other words, if $\mathcal{D}$ is a generalised orbit algebra with generalised orbits $\mathsf{B}_1, \ldots, \mathsf{B}_s$, then for any generalised orbit B_i the polynomial $E_{k,l,r}\,(p_{\mathsf{B}_i})$ is a member of $\mathcal{D}$. We see that :

$$E_{k,l,r}\,(p_{\mathsf{B}_i}) = \sum_{A \ s.t. \ |A|=l} |\{B \in \mathsf{B}_i \ s.t. \ |B \cap A| = r\}|\, p_A$$

As this polynomial is a member of $\mathcal{D}$, we conclude that if B_i and B_j are two generalised orbits of $\mathcal{D}$, then for every set A in B_j, the number of sets in B_i that intersects a subset of size r of A is independent of the choice of A in B_j.

We can also see that in any generalised orbit algebra, the restriction of ∂ to the orbits of size k is injective if $k > \frac{n}{2}$. Indeed by equation 4, we have :

$$E_{k-1,k,t} \circ \partial = E_{k,k,t} + E_{k,k,t+1}, \quad t = 0 \ldots k-1$$

If $k > \frac{n}{2}$, we have $E_{k,k,0} = 0$ and thus :

$$\sum_{t=0}^{k-1} (-1)^{k-1-t} E_{k-1,k,t} \circ \partial = (-1)^{k-1} E_{k,k,0} + E_{k,k,k} = id_k$$

so the restriction of ∂ to the orbits of size k is injective.

As $\partial \circ id_k = E_{k,k-1,k-1}$, we see that $\complement \circ \partial \circ \complement = E_{n-k,n-k+1,n-k+1}$ is injective. With $r = n-k$ this yields that $E_{r,r+1,r}$ is injective if $r < \frac{n}{2}$, and we remark that its transpose in the canonical basis is $E_{r+1,r,r}$ which is then surjective. In any generalised orbit algebra, the number of generalised orbits with cardinality $k+1$ is then at least the number of generalised orbits with cardinality k if $k < \frac{n}{2}$, so to say the Livingstone-Wagner theorem applies.

We shall now investigate further this idea that any two sets in a generalised orbit of a generalised orbit algebra intersect in the same way every generalised orbit of $\mathcal{D}$, by looking at intersection properties of several generalised orbits. If k is a positive integer, we consider the tensor product of k copies of $\mathcal{S}_n$:

$$\mathcal{S}_n^{\otimes k} = \underbrace{\mathcal{S}_n \otimes \ldots \otimes \mathcal{S}_n}_{k}$$

This is a real vector space of dimension 2^{kn}, with the natural basis :

$$p_S = p_{S_1} \otimes \ldots \otimes p_{S_k}, \quad \text{where} \quad S \in \mathcal{P}\,(\Omega)^k$$

Definition 10. *We denote by $Com_k\,(\mathfrak{S}_n)$ the set of linear functions h from $\mathcal{S}_n^{\otimes k}$ to $\mathcal{S}_n$ such that :*

$$\forall \sigma \in \mathfrak{S}_n, \ \sigma \circ h = h \circ (\underbrace{\sigma \otimes \sigma \otimes \ldots \otimes \sigma}_{k})$$

We have already studied the first case ($k = 1$) with $\mathrm{Com}\,(\mathfrak{S}_n)$. As before, the orbits of $\mathfrak{S}_n$ on the $(k+1)$-tuples of subsets of Ω give a basis of $\mathrm{Com}_k\,(\mathfrak{S}_n)$. One can show that the orbit of such a $(k + 1)$-tuple $(S_1, \ldots, S_{k+1})$ is uniquely defined by the function μ_S whose value on every subset J of $\{1, \ldots, k+1\}$ is $\mu_S\,(J) = \left| \bigcap_{j \in J} S_j \right|$. It can be shown that an integer-valued function μ on $\mathcal{P}\,(\{1, \ldots, k+1\})$ is indeed associated with an orbit if and only if

$$\forall J \subseteq \{1, \ldots, k+1\}, \sum_{\substack{L \subseteq \{1, \ldots, k+1\} \\ L \supseteq J}} (-1)^{|L| - |J|} \mu\,(L) \geq 0$$

In this case, we shall say that μ is an *incidence function* of *order $k + 1$*. If a $(k + 1)$-tuple $(S_1, \ldots, S_{k+1})$ is in the orbit defined by such a function μ, we shall write $(S_1, \ldots, S_{k+1}) \vdash \mu$. We can also show that the number of orbits is $\binom{n + 2^{k+1} - 1}{2^{k+1} - 1}$. This enables us to define a basis of $\mathrm{Com}_k\,(\mathfrak{S}_n)$, namely the set of functions

$$E_\mu : p_{S_1} \otimes \ldots \otimes p_{S_k} \mapsto \sum_{A \ s.t \ (S_1, \ldots, S_k, A) \vdash \mu} p_A$$

where μ runs over all the incidence functions of order $k + 1$. One can easily see that the $E_{k,l,r}$ we used previously are indeed the E_μ, with μ running through the incidence functions of order two.

The functions in $\mathrm{Com}_k\,(\mathfrak{S}_n)$ characterise orbit algebras, as :

Theorem 6. *Let $\mathcal{D}$ be a nonempty and nonzero subset of $\mathcal{S}_n$ such that for every positive integer k,*
$$Com_k\,(\mathfrak{S}_n)\,\left(\mathcal{D}^{\otimes k}\right) \subseteq \mathcal{D}$$

Then $\mathcal{D}$ is an orbit algebra.

Proof. It is easy to see that any such set $\mathcal{D}$ is a generalised orbit algebra and that equality holds. As such, it possesses generalised orbits. Let us consider two sets A and B in the same generalised orbit B. It is enough to show that there is a permutation of $\mathfrak{S}_n$ that send A to B, and leaves $\mathcal{D}$ invariant.

If we consider a list $S_1, \ldots, S_{2^n}$ of all the subsets of Ω, and a list $\mathsf{B}_1, \ldots, \mathsf{B}_{2^n}$ of their respective generalised orbits (there might be repetitions), we consider h to be the only basis element of $\mathrm{Com}_{2^n}\,(\mathfrak{S}_n)$ such that $h\,(S_1, \ldots, S_{2^n}) = A$. We have : $h\,\left(\mathcal{D}^{\otimes k}\right) \subseteq \mathcal{D}$, so $h\,(\mathsf{B}_1, \ldots, \mathsf{B}_{2^n})$ is a member of $\mathcal{D}$. It has a nonzero coordinate on B, and we deduce that there exist sets $(T_1, \ldots, T_{2^n})$ such that $T_i \in \mathsf{B}_i$ for every $i = 1 \ldots n$, and $h\,(T_1, \ldots, T_{2^n}) = B$. We claim that there exists a permutation in $\mathfrak{S}_n$ sending S_i to T_i for every i. Such a permutation maps A to B and leaves $\mathcal{D}$ invariant. $\qquad\square$

We shall study the first cases of this closeness property, and as we have already proved that it holds if $k = 1$ for any generalized orbit algebra, we shall now turn to the case $k = 2$.

First, the multiplication m of $\mathcal{S}_n$ is a member of $\mathrm{Com}_2\left(\mathfrak{S}_n\right)$, because every permutation defines an algebra isomorphism, that is, if p and q are two elements of $\mathcal{S}_n$, and σ is a permutation in $\mathfrak{S}_n$, one has : $\sigma\left(p \cdot q\right) = \sigma\left(p\right) \cdot \sigma\left(q\right)$. Also, one can see that if u, v, w are three elements of $\mathrm{Com}\left(\mathfrak{S}_n\right)$, then $\sigma \circ u\left(v(p) \cdot w(q)\right) = u\left(v \circ \sigma\left(p\right) \cdot w \circ \sigma\left(q\right)\right)$, that is, $u \circ m \circ \left(v \otimes w\right)$ is a member of $\mathrm{Com}_2\left(\mathfrak{S}_n\right)$. It is also reassuring to see that for any generalised orbit algebra $\mathcal{D}$, those functions map any element of $\mathcal{D} \otimes \mathcal{D}$ into $\mathcal{D}$. We shall show that the second case of Theorem 6 always hold :

Theorem 7. $\mathrm{Com}_2\left(\mathfrak{S}_n\right)$ *is generated, as a real vector space, by the family :*

$$u \circ m \circ \left(v \otimes w\right), \quad \text{where } u, v, w \ \in Com\left(\mathfrak{S}_n\right)$$

Proof. Let $h = \varepsilon^{-1} \circ m \circ \left(\varepsilon \otimes \varepsilon\right)$ be the only element of $\mathrm{Com}_2\left(\mathfrak{S}_n\right)$ that maps any element $p_A \otimes p_B$ of $\mathcal{S}_n^{\otimes 2}$ to p_A if $A = B$ and to 0 otherwise.
Given any three functions $E_{a_1,k,r_1}, E_{a_2,k,r_2}, E_{k,a_3,r3}$, the function

$$F_{a_1,a_2,a3,r_1,r_2,r_3,k} = E_{k,a_3,r3} \circ h \circ \left(E_{a_1,k,r_1} \otimes E_{a_2,k,r_2}\right)$$

is a linear combination of the functions E_μ, where μ runs over the incidence function of order three defined by $\mu\left(\{i\}\right) = a_i$ for $i = 1, 2, 3$. We shall show that for a given triple $\left(a_1, a_2, a_3\right)$ of numbers between 0 and n, this linear system gives the E_μ.

Given a member $\left(A_1, A_2, A_3\right)$ of the orbit represented by μ, the coefficient of the decomposition of $F_{a_1,a_2,a3,r_1,r_2,r_3,k}$ on E_μ is the number of subsets U of Ω such that :

$$\begin{aligned}
|U| &= k \\
|U \cap A_1| &= r_1 \\
|U \cap A_2| &= r_2 \\
|U \cap A_3| &= r_3
\end{aligned}$$

If such a set U exists, one must have :

$$|U \cap \left(A_1 \cup A_2\right)| = |U \cap A_1| + |U \cap A_2| - |U \cap A_1 \cap A_2| \le |U|$$

that is to say :

$$r_1 + r_2 - k \le |U \cap A_1 \cap A_2| \le |A_1 \cap A_2| = \mu\left(\{1, 2\}\right)$$

Likewise, we have :
$$r_1 + r_3 - k \le \mu\left(\{1, 3\}\right)$$
$$r_2 + r_3 - k \le \mu\left(\{2, 3\}\right)$$

In the same manner, considering $U \cap \left(A_1 \cup A_2 \cup A_3\right)$, one can see that :

$$|U \cap A_1| + |U \cap A_2| + |U \cap A_3| - |U \cap A_1 \cap A_2| - |U \cap A_1 \cap A_3| - |U \cap A_2 \cap A_3| + |U \cap A_1 \cap A_2 \cap A_3| \le |U|$$

That is :

$$
\begin{aligned}
r_1 + r_2 + r_3 - k \;\; \leq \;\; & |U \cap A_1 \cap A_2 \cap A_3^c| + |U \cap A_1 \cap A_2^c \cap A_3| + |U \cap A_1^c \cap A_2 \cap A_3| \\
& + 2|U \cap A_1 \cap A_2 \cap A_3| \\
\leq \;\; & |A_1 \cap A_2 \cap A_3^c| + |A_1 \cap A_2^c \cap A_3| + |A_1^c \cap A_2 \cap A_3| + 2|A_1 \cap A_2 \cap A_3| \\
\leq \;\; & \mu\left(\{1,2\}\right) + \mu\left(\{1,3\}\right) + \mu\left(\{2,3\}\right) - \mu\left(\{1,2,3\}\right)
\end{aligned}
$$

We summarize these inequalities in matrix form :

$$
\begin{bmatrix} 1 & 1 & 0 & -1 \\ 0 & 1 & 1 & -1 \\ 1 & 0 & 1 & -1 \\ 1 & 1 & 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} r_1 \\ r_2 \\ r_3 \\ k \end{bmatrix} \leq \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} \mu\left(\{1,2\}\right) \\ \mu\left(\{1,3\}\right) \\ \mu\left(\{2,3\}\right) \\ \mu\left(\{1,2,3\}\right) \end{bmatrix}
$$

It can be checked that the two matrices are invertible. Thus, given a_1, a_2, a_3, if we consider two convenient orders on r_1, r_2, r_3, k and on the incidence functions μ such that $\mu\left(\{i\}\right) = a_i$, the expression of the $F_{a_1, a_2, a_3, r_1, r_2, r_3, k}$ on the E_μ is triangular[3], and one can see that this system is invertible, that is to say the diagonal elements are non-zero, by considering $U = (A_1 \cap A_2) \cup (A_2 \cap A_3) \cup (A_1 \cap A_3)$ with the previous notations.

□

We would like to use the same strategy to obtain $\mathrm{Com}_3\left(\mathfrak{S}_n\right)$, using linear combinations of functions such as $u \circ (v \otimes id)$ where u and v range over $\mathrm{Com}_2\left(\mathfrak{S}_n\right)$, but this is not possible. In fact, the dimension of the linear hull of such functions is bounded above by three times the squared dimension of $\mathrm{Com}_2\left(\mathfrak{S}_n\right)$, that is $3\binom{n+7}{7}^2$, whereas the dimension of $\mathrm{Com}_3\left(\mathfrak{S}_n\right)$ is $\binom{n+15}{15}$. Hence, if n is large enough :

$$
3\dim\left(\mathrm{Com}_2\left(\mathfrak{S}_n\right)\right)^2 < \dim \mathrm{Com}_3\left(\mathfrak{S}_n\right)
$$

Theorem 7 has an interesting consequence : for any generalised orbit algebra $\mathcal{D}$, we have $\mathrm{Com}_2\left(\mathfrak{S}_n\right)\left(\mathcal{D} \times \mathcal{D}\right) = \mathcal{D}$. We can define $\mathcal{D}$ to be a subalgebra of functions of $\mathcal{S}_n$ to itself, via multiplication. Theorem 7 asserts that this algebra is closed under transposition, and thus completely determined by its commutant.

3   Reconstruction problems

Generalised orbit algebras are strongly related to reconstruction conjectures in graph theory. We state the vertex and edge reconstruction conjectures separately, as they illustrate two distinct points of view on the possible use of generalised orbit algebras in reconstruction problems. We first recall the necessary definitions, the interested reader being invited to refer to [1] for a survey of reconstruction results, and to [2] for an introduction to graph theory.

---

[3]to be exact, a subsystem is triangular

Let $V = \{1, \ldots, f\}$, and let E be the set of all subsets of V of size two. We shall call V the set of *vertices*, and *edges* the elements of E. We define a *graph* to be a subset of E, and call E the *complete graph*, whereas the empty set will be the *empty graph*. We also define a *subgraph* of a graph G to be any subset of G. The elements of G will be called the edges of G, an edge $\{i, j\}$ of G being said *incident* to the vertices i and j.

For example, if $f = 3$, we can represent the complete graph on three vertices, one of its subgraphs, and an edge incident to the vertices 1 and 2.
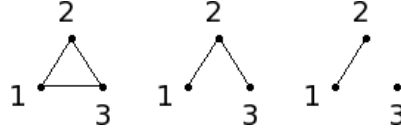
The group $\mathfrak{S}_V$ of permutations of the set V acts on E with the natural action $\sigma \cdot \{i, j\} = \{\sigma \cdot i, \sigma \cdot j\}$. Likewise, we can lift this action of $\mathfrak{S}_V$ on edges to the set of all graphs. We will say that two graphs G and H are *isomorphic* if they are in the same orbit for this action. We shall denote by $[G]$ the orbit of the graph G. For example, if $f = 3$, the permutation (12) acts as follows :
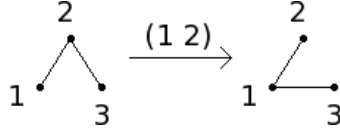
Together with the following graph, these two graphs form an orbit of $\mathfrak{S}_V$:
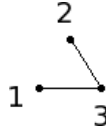
3.1 Vertex-reconstruction conjecture

For a graph G, and a vertex v, we define the *vertex-deleted subgraph* $G - v$ as the subgraph of G that contains every edge of G not incident to v. Two graphs G and H on the same vertex set V are called *hypomorphic* if, for each $v \in V$, the subgraphs $H - v$ and $G - v$ are isomorphic. A *reconstruction* of a graph G is a graph that is hypomorphic to G. A graph G is said to be *reconstructible* if every reconstruction of G is isomorphic to G.

Conjecture 1 (Kelly-Ulam [17]). *Every graph on at least three vertices[4] is reconstructible.*

---

[4]with our notations $f \geq 3$

For every edge $\{i, j\}$ of E, we define a variable $x_{i,j}$, and define the algebra $\mathcal{G}_f$ to be the quotient of the real polynomials $\mathbb{R}[x_{\{1,2\}}, \ldots, x_{\{f-1,f\}}]$ by the ideal generated by the elements :

$$x_{\{1,2\}}^2 - x_{\{1,2\}}, x_{\{1,3\}}^2 - x_{\{1,3\}}, \ldots, x_{\{f-1,f\}}^2 - x_{\{f-1,f\}}$$

We reproduce here the algebraic point of view of the first part, in the particular case of graphs, that is to say, when $\Omega = E$. The real vector space $\mathcal{G}_f$ have dimension $2^{\binom{f}{2}}$, and the polynomials

$$p_G = \prod_{\{u,v\} \in G} x_{\{u,v\}}$$

where G is a graph, are a basis of $\mathcal{G}_f$. We have seen that the group of permutations of V $\mathfrak{S}_V$ acts on $\mathcal{G}_f$ as a group of algebra isomorphisms (subgroup of the group of permutations $\mathfrak{S}_E$). Consequently, we can consider the algebra of its invariants $\mathcal{G}_f^{\mathfrak{S}_V}$. It is clear that this is a vector space with basis

$$p_{[G]} = \sum_{G \in [G]} p_G$$

where $[G]$ runs over every isomorphism class of graphs. If we define by linearity the evaluation of a polynomial p_G on a graph H to be :

$$p_G(H) = \begin{cases} 1 & \text{if } G \subseteq H \\ 0 & \text{otherwise} \end{cases}$$

then $p_{[G]}(H)$ is simply the number of subgraphs of H that are isomorphic to G.

An *isolated vertex* of a graph G is a vertex which is incident to no edge of G, we denote by iv (G) the number of isolated vertices in G. If we now consider the set $\mathcal{I}_f$ of polynomials $p_{[G]}$ in $\mathcal{G}_f$, where $[G]$ runs over all the isomorphism classes of graphs with at least one isolated vertex, then H is a reconstruction of G if and only if $p(G) = p(H)$ for every polynomial p in $\mathcal{I}_f$, for :

Lemma 5 (Kelly). *If F is a graph with at least one isolated vertex, then for every graph G :*

$$p_{[F]}(G) = \frac{1}{iv(F)} \sum_{v \in V} p_{[F]}(G - v)$$

Knowing the values of the polynomials p of $\mathcal{I}_f$ on G allows us to know the list of the vertex deleted subgraphs $G - v$ up to isomorphism. Thus, the generalised orbits of the partition of the set of graphs associated with the algebra generated by $\mathcal{I}_f$ in Theorem 3 are the classes of hypomorphic graphs. We deduce that Conjecture 1 is equivalent to :

Conjecture 2. *If f is at least three, then the subalgebra of $\mathcal{G}_f$ generated by the polynomials of $\mathcal{I}_f$ is $\mathcal{G}_f$ itself.*

17

Thus we can split the Kelly-Ulam Conjecture [5] into three parts :
for $f \geq 3$,

- The subalgebra of $\mathcal{G}_f$ generated by the polynomials of $\mathcal{I}_f$ is a generalised orbit algebra.

- This generalised orbit algebra is an orbit algebra.

- The stabilizer of this algebra is $\mathfrak{S}_V$.

We can easily address the third one, that is to say the group of permutations of the edges that leave invariant every polynomial of $\mathcal{I}_f$ is $\mathfrak{S}_V$. To show this, we note that a permutation of $\mathfrak{S}_E$ that leaves any polynomial of $\mathcal{I}_f$ invariant also leaves invariant the polynomial :

$$g = \sum_{i=1}^{f} \prod_{\substack{j=1 \\ j \neq i}}^{n} x_{\{i,j\}}$$

because $\complement(g)$ is in $\mathcal{I}_f$.

A consequence of the definition of the action of $\mathfrak{S}_E$ on $\mathcal{G}_f$ is that such permutations permute the

$$s_i = \prod_{\substack{j=1 \\ j \neq i}}^{n} x_{\{i,j\}}$$

This yields a one to one correspondence between the permutations of E that leave g (i.e. $\mathcal{I}_f$) invariant, and the permutations of V.

Observe that if the second point is true the generalised orbit algebra should be generated by g [6]. It is clear that the vertex reconstruction conjecture implies the second point. But one can also show :

Theorem 8. *If the vertex reconstruction conjecture is true, then the generalised orbit algebra generated by g is the orbit algebra of graphs.*

Proof. We prove that for every type of graph $[G]$, $p_{[G]}$ is in the generalised orbit algebra generated by g, by induction on the number of non-isolated vertices of G. We have seen that $p_\emptyset = 1$ is in every generalised orbit algebra, just like the polynomial associated with graphs of size one, that is to say edges. Now if we consider an isomorphism class of graph $[G]$ with $t+1$ non-isolated vertices ($t \geq 2$), we know by the induction hypothesis that the polynomials $p_{[H]}$, where H is a graph with at most t non-isolated vertices, are elements of the generalised orbit algebra generated by g. By the reformulation of Conjecture 1 as Conjecture 2 (with $f = t+1$), there exists a polynomial $r_{[G]}$ in the generalised orbit algebra

---

[5] conjecture 1

[6] As the intersection of two generalised orbit algebras is a generalised orbit algebra, we may consider the generalised orbit algebra generated by g to be the smallest generalised orbit algebra containing g.

18

generated by g, that takes the same value as $p_{[G]}$ on every graph with at most $t + 1$ non-isolated vertices. Observe that $r_{[G]}$ is equal to $p_{[G]}$ plus a sum of $\alpha_{[H]}p_{[H]}$, where $[H]$ runs through the isomorphism classes of graphs with at least $t + 2$ non-isolated vertices. We conclude by eliminating these terms as follows :

- First we generate the polynomial p_{t+1} corresponding to the cliques of size $t + 1$ as a member of the generalised orbit algebra generated by g.

- Then we note that for any graph H with less than $t + 1$ non isolated vertices :
$$\varepsilon_H \cdot (\varepsilon \circ l(p_{t+1})) = \binom{\mathrm{iv}(H)}{f - t - 1}\varepsilon_H$$
  and that the left hand side is otherwise zero.

- Finally, we consider $\varepsilon^{-1}\left(\varepsilon(r_G) \cdot (\varepsilon \circ l(p_{t+1}))\right)$.

$\square$

As infinite families of non-reconstructible digraphs exist (see [16]), we briefly look at what happens in this case. Instead of considering Ω to be the set of all two element subsets of $\{1, \ldots, f\}$, we consider it to be the set P of ordered pairs of distinct elements. The group of permutations $\mathfrak{S}_V$ acts on P by $\sigma \cdot (i, j) = (\sigma \cdot i, \sigma \cdot j)$. One can then ask whether the polynomials corresponding to isomorphism classes of digraphs with at least one isolated vertex generate the whole orbit algebra.

- if $f = 3$, the algebra generated by the polynomials corresponding to types of digraphs with at least one isolated vertex is a generalised orbit algebra, and an orbit algebra, but the stabilizer also switches edges directions.

- if $f = 4$, the algebra is not a generalised orbit algebra. Consider the following two hypomorphic digraphs: there are no other digraph hypomorphic to them :

  Both of these digraphs contain the second of the following two digraphs, but not the first.

Those last two digraphs are nevertheless hypomorphic, and there are no other digraph hypomorphic to them. We see here that the number of subdigraphs with a given deck is not reconstructible, which implies that the algebra generated by the polynomials corresponding to types of digraphs with at least one isolated vertex is not a generalised orbit algebra

3.2 Edge-reconstruction conjecture

If G is a graph, a graph H is said to be an *edge-reconstruction* of G if there is a bijection ϕ between the edges of G and the edges of H such that for every edge u of G, $G - u$ and $H - \phi(u)$ are isomorphic. The graph G is said to be *edge-reconstructible* if every edge-reconstruction of G is isomorphic to G.

Conjecture 3 (Harary[7])**.** *Every graph on at least four edges is edge-reconstructible.*

We take the opportunity here to emphasize the structure coefficients of a generalised orbit algebra. Recall that there is a partition of $\mathcal{P}\left(\Omega\right)^7$ associated with any generalised orbit algebra by Theorem 3, that is both a basis of the generalised orbit algebra, and the list of sets on which the polynomials in the generalised orbit algebra take constant values. We deduce that for any generalised orbit algebra $\mathcal{D}$ whose system of generalised orbits is $\mathsf{B}_1, \ldots, \mathsf{B}_s$, one can define, for any two generalised orbits B_i and B_j, and any member A of B_i :

$$\binom{\mathsf{B}_i}{\mathsf{B}_j} = |\{B \subseteq A \ s.t. \ B \in \mathsf{B}_j\}|$$

as this number is independent of the choice of A in B_i (we might use the different notations $\binom{A}{\mathsf{B}_j}$ or even $\binom{A}{B}$ for this number). These coefficients encode structure of the generalised orbit algebra $\mathcal{D}$ in the following sense :

- We consider the list of the generalised orbits of the generalised orbit algebra to be such that the matrix C is known, for example with $p_{\mathsf{B}_i^c} := \mathsf{C}\left(p_{\mathsf{B}_i}\right) = p_{\mathsf{B}_{s-i}}$.

- The matrix of ∂ with respect to the basis $p_{\mathsf{B}_1}, \ldots, p_{\mathsf{B}_s}$ has coefficient $[\mathsf{B}_i, \mathsf{B}_j]$ equal to $\binom{\mathsf{B}_i^c}{\mathsf{B}_j^c}$ if $\sharp\mathsf{B}_i = \sharp\mathsf{B}_j - 1$ and 0 otherwise.

- The multiplication rule is given by

$$p_{\mathsf{B}_i} \cdot p_{\mathsf{B}_j} = \sum_{k=1}^{s} \binom{\mathsf{B}_k}{\mathsf{B}_i, \mathsf{B}_j} p_{\mathsf{B}_k}$$

where the coefficient $\binom{\mathsf{B}_k}{\mathsf{B}_i, \mathsf{B}_j}$ can be computed via Möbius inversion :

$$\binom{\mathsf{B}_k}{\mathsf{B}_i, \mathsf{B}_j} = \sum_{l=1}^{s} (-1)^{\sharp\mathsf{B}_k - \sharp\mathsf{B}_l} \binom{\mathsf{B}_k}{\mathsf{B}_l} \binom{\mathsf{B}_l}{\mathsf{B}_i} \binom{\mathsf{B}_l}{\mathsf{B}_j}$$

---

[7]called system of generalised orbits

For any generalised orbit algebra $\mathcal{D}$, we define a *coefficient matrix* to be a matrix indexed by a list of generalised orbits $(\mathsf{B}_1, \ldots, \mathsf{B}_s)$ of $\mathcal{D}$, and with coefficient $[i,j]$ equal to $\binom{\mathsf{B}_i}{\mathsf{B}_j}$.

A Gap ([5]) experiment shows that an orbit algebra of order smaller than 9 is uniquely defined up to conjugation by its coefficient matrix. It is then natural to look at which matrices are indeed coefficient matrices of a generalised orbit algebra. We can easily state a number of relations between coefficients. For example, a simple counting argument gives :

$$\binom{\Omega}{\mathsf{B}_i}\binom{\mathsf{B}_i^c}{\mathsf{B}_j^c} = \binom{\Omega}{\mathsf{B}_j}\binom{\mathsf{B}_j}{\mathsf{B}_i}$$

We can also see that the coefficient matrix $\mathcal{M}$ is the matrix of $\mathsf{C} \circ l \circ \mathsf{C}$. We can now reformulate Lemma 2 in its original form ([13]), that is to say, for every nonzero integer m :

$$\mathcal{M}_{[i,j]}^m = m^{\sharp \mathsf{B}_i - \sharp \mathsf{B}_j} \mathcal{M}_{[i,j]} \tag{7}$$

With the study of the $\mathrm{Com}_k(\mathfrak{S}_n)$, we have already defined many relations :

- relations that result from the definition of $\mathrm{Com}(\mathfrak{S}_n)$ as the algebra generated by ∂ and C.

- composition relations between the elements of the basis of $\mathrm{Com}(\mathfrak{S}_n)$.

- linear combinations between the $u \circ m \circ (v \otimes w)$, where u, v, w runs through the $E_{k,l,r}$ (i.e. a basis of $\mathrm{Com}(\mathfrak{S}_n)$).

- although we do not know how to generate $\mathrm{Com}_k(\mathfrak{S}_n)$ if $k \geq 3$, some linear relations might arise between the functions that we do know how to generate.

As we can see, the framework of the commutants $(\mathrm{Com}(\mathfrak{S}_n), \mathrm{Com}_k(\mathfrak{S}_n))$ generates ex-nihilo some polynomial relations between the coefficients of a generalised orbit algebra. We might ask whether they can be useful towards reconstruction problems. First, we follow [3] and rephrase the Edge Reconstruction Conjecture 3 in the more general framework of orbit algebras.

Given a group Γ of permutations of Ω, we say that two subsets A and B of Ω are Γ-*isomorphic* if there is an element σ of Γ such that $\sigma \cdot A = B$. If A and B are two subsets of Ω and there is a bijection ϕ from A to B such that for every e in A, the subsets $A - e$ and $B - \phi(e)$ are Γ-isomorphic, we say that B is a Γ-*reconstruction* of A. A is said to be Γ-*reconstructible* if every Γ-reconstruction of A is isomorphic to A. We would like to know which sets are Γ-reconstructible ? There is a version of Kelly's Lemma for this problem :

Lemma 6 (Kelly). *If A and C are two subsets of Ω such that $|C| < |A|$, then :*

$$\binom{A}{C} = \frac{1}{|A| - |C|} \sum_{e \in A} \binom{A - e}{C}$$

It is then clear that requiring that two sets A and B satisfy the condition that $A - e$ is isomorphic to $B - \phi(e)$ for every element e of A is equivalent to requiring that, for every set C with fewer than $|A|$ elements,

$$\binom{A}{C} = \binom{B}{C}$$

Note also that Kelly's Lemma apply for generalised orbit algebras. One can show that the relations stated in this result are exactly the same as the ones obtained in equation (7), that is to say, a coefficient matrix satisfying one set of relations satisfies the other set.

We now look at the first relation obtained with the generalised orbit algebra structure. From equations (5) or (6), we deduce that for any generalised orbit algebra $\mathcal{D}$, and for any two generalised orbits B_1 and B_2 of $\mathcal{D}$ with sizes k and l respectively, the coefficient of the matrix of $E_{k,l,r}$ is :

$$E_{k,l,r_{[\mathsf{B}_1,\mathsf{B}_2]}} = \sum_{\mathsf{U}} (-1)^{|\mathsf{U}|-r} \binom{|\mathsf{U}|}{r} \binom{\mathsf{B}_1}{\mathsf{U}} \binom{\mathsf{U}^c}{\mathsf{B}_2^c}$$

where the sum runs over every generalised orbit U of $\mathcal{D}$. Observe that this should be 0 if $k + l - r > n$. Thus if B_1 and B_2 are two generalised orbits both of size $k > \frac{n}{2}$ such that for every generalised orbit U distinct from B_1 or B_2 we have $\binom{\mathsf{B}_1}{\mathsf{U}} = \binom{\mathsf{B}_2}{\mathsf{U}}$, then

$$
\begin{aligned}
E_{k,k,0_{[\mathsf{B}_1,\mathsf{B}_1]}} - E_{k,k,0_{[\mathsf{B}_2,\mathsf{B}_1]}} &= \sum_{\mathsf{U}} (-1)^{|\mathsf{U}|} \left(\binom{\mathsf{B}_1}{\mathsf{U}} - \binom{\mathsf{B}_2}{\mathsf{U}} \right) \binom{\mathsf{U}^c}{\mathsf{B}_1^c} \\
&= (-1)^{|\mathsf{B}_1|}
\end{aligned}
$$

Since $E_{k,k,0}$ is the zero mapping we have a contradiction. We deduce that :

Theorem 9 (Lovász [9][3])**.** *For every group Γ of permutations of Ω, if A and B are two subsets of Ω and there is a bijection ϕ from A to B such that for every e in A, $A - e$ and $B - \phi(e)$ are Γ-isomorphic, and if the size of A is bigger than $\frac{n}{2}$, then A and B are Γ-isomorphic.*

This result also applies to generalised orbit algebras, if one replaces the notion of isomorphism by membership in the same generalised orbit. This theorem is in some sense best possible in the general framework of orbit algebras, and consequently, also for generalised orbit algebras. Indeed, there exists orbit algebras of order $2r$ with non reconstructible sets of size r. As an example, consider the orbit algebra of the permutation group Γ generated by :

$$\{(1,2)(2i+1, 2i+2), \quad i = 1..r-1\}$$

Consider the set $U = \{2i, \ i = 2 \ldots r\}$, and let $A = U \cup \{1\}$, $B = U \cup \{2\}$. We now have two sets A and B of size r not in the same orbit of Γ, because every element of Γ leaves invariant the parity of the number of even elements of

sets containing exactly one element in each pair $\{2i+1, 2i+2\}$, $i = 0 \ldots r-1$. However, if one considers a subset[1] of size $r-1$ in A, then one can see that there exists exactly one pair $\{2j+1, 2j+2\}$ with no element in A, and applying $(1,2)(2j+1, 2j+2)$ we find a subset[1] of size $r-1$ in B. This defines a one to one mapping from the subsets of size $r-1$ in A to the subsets of size $r-1$ in B , showing that B is a Γ-reconstruction of A.

For the sake of completeness, one can add the element $2r+1$, and get an algebra of order $2r+1$ with non-reconstructible sets of size r.

It is therefore natural to try to find properties of the group that would allow us to lower the bound of $\frac{n}{2}$. Considering the order of the group yields a theorem of V.Müller that also applies in any generalised orbit algebra (even if there is no group to consider). We prove a slightly different result in the more general context of generalised orbit algebras :

Theorem 10. *If $\mathcal{D}$ is a generalised orbit algebra of order n with generalised orbits $\mathsf{B}_1, \ldots, \mathsf{B}_s$, and A and B are two subsets of Ω with cardinality k, such that for every generalised orbit B_i of size less than k, $\binom{A}{\mathsf{B}_i} = \binom{B}{\mathsf{B}_i}$, then for every generalised orbit B_j :*

$$2^{k-|\mathsf{B}_j|-1} \leq \binom{\mathsf{B}_j^c}{A^c}$$

Proof. Let A be a set and B, S generalised orbits, then

$$E_{A,B}^S = \sum_{V \in \mathsf{B}} (-1)^{|V|-|S|} \binom{V}{S}\binom{A}{V}\binom{V^c}{B^c}$$

is the number of graphs whose intersection with A is exactly a copy of S, and that are elements of B.

We have :

$$\sum_S \binom{S}{T} E_{A,B}^S = \binom{A}{T}\binom{T^c}{B^c}$$

and if B is a reconstruction of A:

$$
\begin{aligned}
E_{A,A}^T - E_{B,A}^T &= \sum_{V \in \mathsf{B}} (-1)^{|V|-|T|} \binom{V}{T}\left(\binom{A}{V} - \binom{B}{V}\right)\binom{V^c}{A^c} \\
&= (-1)^{|A|-|T|}\binom{A}{T}
\end{aligned}
$$

---

[1] distinct from U

23

so

$$2^{|A|-|S|}\binom{A}{S} \;=\; \sum_T \binom{T}{S}|E_{A,A}^T - E_{B,A}^T|$$

$$\leq\; \sum_T \binom{T}{S}E_{A,A}^T + \sum_T \binom{T}{S}E_{B,A}^T$$

$$\leq\; \binom{A}{S}\binom{S^c}{A^c} + \binom{B}{S}\binom{S^c}{A^c}$$

hence, if S contains a strict subset of A (thus, of B), we have :

$$2^{|A|-|S|-1} \leq \binom{S^c}{A^c}$$

$\square$

Using $\mathsf{B}_j = \{\emptyset\}$ we get :

Corollary 2 (Müller [14]). *If $\mathcal{D}$ is a generalised orbit algebra of order n with generalised orbits $\mathsf{B}_1, \ldots, \mathsf{B}_s$, and A and B are two subsets of Ω with cardinality $k > 1 + \log_2 \binom{\Omega}{A}$, such that for every generalised orbit B_i of size less than k, $\binom{A}{\mathsf{B}_i} = \binom{B}{\mathsf{B}_i}$, then A and B belong to the same generalised orbit of $\mathcal{D}$.*

In the case of the orbit algebra of the group Γ, this implies that sets of size greater than $1+\log_2 |\Gamma|$ are Γ-reconstructible (see [3]). In the above example, the group Γ is commutative, and of order 2^{r-1}, so $1 + \log_2(\Gamma) = r$: this example also shows that Müller's theorem is best possible. By adding an appropriate number of (fixed) elements, one can construct a subgroup of $\mathfrak{S}_n$ of order 2^{r-1} with non-reconstructible subsets of size r, if $n \geq 2r$. Thus, all the limit cases of Müller's theorem are covered, because if $n < 2r$, we know by Lovász's theorem that sets of size r are reconstructible. This example shows that one cannot use the polynomial relations between the coefficients of generalised orbit algebras to improve Theorems 9 and 2 without introducing another generalised orbit algebra parameter than the maximum size of a generalised orbit.

As an example, one can consider the following :

Corollary 3 (Maynard-Siemons [10]). *If Γ acts freely on Ω, then the reconstruction index of Γ, defined as the least cardinality for which every set is Γ-reconstructible, is at most 5.*

Proof. Using B_j as a convenient orbit of cardinality 1, we have $2^{|A|-2} \leq \dfrac{\binom{\Omega}{A}}{\binom{\Omega}{\mathsf{B}_j}}\binom{A}{\mathsf{B}_j}$. As Γ acts freely we have $|\Gamma| = \binom{\Omega}{\mathsf{B}_j} \geq \binom{\Omega}{A}$. We deduce that $2^{|A|-2} \leq |A|$, so $|A| \leq 4$. $\square$

We refer to [10] for a complete classification of freely acting groups with respect to their reconstruction index.

3.3 Generalised orbit algebras are not orbit algebras

To construct generalised orbit algebras not arising from a group of permutations, we go back to Theorem [9], and remark that according to the proof, any two sets A and B such that for every orbit distinct from A and B $\binom{A}{C} = \binom{B}{C}$ have size equal to r only if either :

- elements of A and B are complements of each other, or

- A and B are self-complementary

There exists invariant algebras for both cases, in the above example, the orbits of A and B are :

- complements of each other if r is odd

- both self complementary if r is even

In these conditions, we remark that unifying the generalised orbits A and B yields a generalised orbit algebra. Sometimes, the resulting generalised orbit algebra may not be an orbit algebra, that is to say, for the first orbit algebra, there's not always an outer permutation stabilizing every orbit except A and B, but mixing elements of A and B.

For example, if $n = 8$ and Γ is the group generated by the permutations

$$(1,2)(3,4),\ (5,6)(7,8),\ (1,3,2,4)(5,7,6,8),\ (1,5)(2,6)(3,7)(4,8)$$

we take $A = \{1,3,5,7\}$ and $B = \{1,3,5,8\}$. A can be written as the union of two sets in the same orbit O : $\{1,3,7\}$ and $\{3,5,7\}$, with intersection $\{3,7\}$, whereas B can be written only in one way as the union of two sets of O : $\{1,3,8\}$ and $\{1,5,8\}$, but the intersection $\{1,8\}$ is not in the same orbit as $\{3,7\}$.

This is in contradiction with the fact that there can be a permutation mapping $\{1,3,5,7\}$ to $\{1,3,5,8\}$ respecting the orbits of $\{1,3,7\},,\{3,7\}$, and $\{1,8\}$. Thus, the resulting generalised orbit algebra is not an orbit algebra, as it is not "closed" under $\mathrm{Com}_3\left(\mathfrak{S}_n\right)$, in the sense of Theorem 6.

Acknowledgements

References

[1] J.A.Bondy, A graph reconstructor's manual. *Surveys in Combinatorics* (1991) **166** 221-252

[2] J.A.Bondy U.S.R.Murty, Graph Theory. *Graduate Texts in Mathematics* **244** Springer (2007)

[3] P.J.Cameron, Stories from the age of reconstruction.*Congressus Numerantium* **113** (1996) 31-41

[4] P.J.Cameron P.M.Neumann J.Saxl, On groups with no regular orbits on the set of subsets. *Archiv der Mathematik* **43** (1984) no. 4, 295-296.

[5] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4.12*; 2008, (\protect\vrule width0pt\protect\href{http://www.gap-system.org}{http://www.gap-system.o

[6] J.T.Go, The Terwilliger algebra of the hypercube. *European J. Combin.* **23** (2002) no.4. 399-429

[7] F.Harary, On the reconstruction of a graph from a collection of subgraphs. *Theory of graphs and its applications* (1964)

[8] D.Livingstone A.Wagner, Transitivity of finite permutation groups on unordered sets. *Mathematische Zeitschrift* **90** (1965) 393-403

[9] L.Lovász, A note on the line reconstruction problem. *J. Combin. Theory Ser. B* **13** (1972) 309-310

[10] P.Maynard J.Siemons, On the reconstruction index of permutation groups : semiregular groups. *Aequationes Math.* **64** (2002) 218-231

[11] P.Maynard J.Siemons, On the reconstruction index of permutation groups : general bounds. *Aequationes Math.* **70** (2005) 225239

[12] V.B.Mnukhin, An introduction to Möbius algebras. *Tempus Lecture notes* **11**

[13] V.B.Mnukhin, The k-orbit reconstruction and the orbit algebra. *Acta Applic. Math.* **29** (1992) 83-117

[14] V.Müller, The edge reconstruction hypothesis is true for graphs with more then $n \log_2 n$ edges. *J. Combin. Theory Ser. B* **22** (1977) 281-283

[15] A.Schrijver, New code upper bounds from the Terwilliger algebra and semidefinite programming. *IEEE Trans. Inform. Theory* **51** (2005), no. 8, 2859-2866

[16] P.K.Stockmeyer, A census of nonreconstructible digraphs.I. Six related families. *J.Combin.theory Ser. B* (1981) **31** 232-239

[17] S.M.Ulam, A Collection of Mathematical Problems. Wiley (Interscience), New York (1960) **29**